United States Patent and Trademark Office

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/883,733	06/18/2001	Alexander E. Andreev	01-308 1496.00129	2457

24319 7590 02/23/2005

LSI LOGIC CORPORATION
1621 BARBER LANE
MS: D-106
MILPITAS, CA 95035

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 02/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/883,733	**Applicant(s)** ANDREEV ET AL.	
	Examiner Samson B Lemma	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-20** have been examined.

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. **Claims 1-10** are rejected under 35 U.S.C. 101 because the subject matter is directed to non-statutory subject matter.

4. **Claims 1-10** are directed to a method of defining a transformation between an input signal and an output signal by allocating input signal and establishing a plurality of transfer functions each configured to present a plurality of unique symbols as a block output signal and finally concatenating said block signals to form output signal. The examiner asserts that the limitation of the claims does not fall within the statutory classes listed in 35 USC 101. The language of the claims raises a question as to whether the claims are directed merely to an abstract idea that is not tied to a technological art, environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. **Claims 1-2,7-10,11-12,17-20** are rejected under 35 U.S.C. 102 (b) as being anticipated by **Terry F. Ritter** (hereinafter refereed to as **Ritter**) (U.S. Patent No. 5,623,549)

7. **As per claim 1, 11 and 20 Ritter** discloses a method of defining a transformation between an input signal and an output signal, the method comprising the steps of:

- (A) **Allocating said input signal** [Column 16, lines 64-65; Figure 10, ref. Num "106"](64 bit-input message block X is allocated) **among a plurality of block input signals**[Column 16, lines 65-66; Figure 10, ref. Num "183a"](the input message is allocated into eight message sub-blocks x1, x2,......,x8 where each x_i is an 8 bit sub-block of X);
- (B) **Establishing a plurality of transfer functions configured to present a plurality of unique symbols as a block output signal responsive to said block input signal;** [Column 16, lines 66-column 17, lines 6; figure 10,ref. Num "182" shown above ref. Num "180"; ref. Num "180"; ref. Num "182" shown below ref Num "180"](Each of the blocks $\mathbf{x_i}$ is transformed first via corresponding substitution mechanism or transfer function as shown on figure 10, ref. Num "182" which is shown above ref. Num "180" to produce an 8 bit values $\mathbf{x'_i}$. Then the 8-bit data values $\mathbf{x'_i}$ as a 64 bit data block goes to

another transfer function which is the DES mechanism shown on figure 10, ref. Num "180" and using the **key K** produces a 64-bit output data block **Y** made up of 8-bit sub-blocks y1, y2, y3....y8 .Finally each of the 8-bit sub-**blocks** $\mathbf{y_i}$ is transformed again by a substitution/transfer function block as shown on figure 10, ref. Num "182" below ref. Num "180" and produces 8-bit data block output $\mathbf{y'_1}$)

- **(C) concatenating said block output signals to form said output signal**.[Column 17, lines 6-8]

8. **As per claim 2 and 12 Ritter** discloses the method of defining a transformation between an input signal and an output signal as applied to claim 1 and 11 above. Furthermore **Ritter** discloses the method wherein step (C) **is concatenating said block output signals to form an intermediate result,** [Figure 10, ref. Num "n" just above ref. Num "180"](The output signal after they are permuted for the 1st time, the ouput is concatenated just before they are encrypted again by the DES Key inside the cipher mechanism shown on figure 10, ref. Num "180") the method further comprising **the step of establishing a second transfer function configured to permutate said intermediate result to present said output signal.**[Figure 10, ref. Num "182" which si shown at the below ref. Num "180" and ref. Num "108"][See also Column 16, lines 66-column 17, lines 8]

9. **As per claim 7,8, 17 and 18 Ritter** discloses the method of defining a transformation between an input signal and an output signal as applied to claim 1 and 11 above. Furthermore **Ritter** discloses the method wherein wherein step (A) is allocating a predetermined number of units of said input signal to each said block input signal.[Column 16, lines 63-66] (The 64-bit

input message or signal is allocated into eight message sub-blocks where each is 8-bit sub-blocks.)

10. **As per claim 9,10 and 19 Ritter** discloses the method of defining a transformation between an input signal and an output signal as applied to claims 1 and 11 above. Furthermore **Ritter** discloses the method wherein wherein the steps of duplicating said counter and said plurality of transfer functions to produce a plurality of output signals; [Column 16, lines 66-column 17, lines 6; figure 10,ref. Num "182" shown above ref. Num "180"; ref. Num "180"; ref. Num "182" shown below ref Num "180"](Each of the blocks **x_i** is transformed first via corresponding substitution mechanism or transfer function as shown on figure 10, ref. Num "182" which is shown above ref. Num "180" to produce an 8 bit values **x'_i**. Then the 8-bit data values **x'_i** as a 64 bit data block goes to another transfer function which is the DES mechanism shown on figure 10, ref. Num "180" and using the **key K** produces a 64-bit output data block **Y** made up of 8-bit sub-blocks y1, y2, y3....y8 .Finally each of the 8-bit sub-**blocks y_i** is transformed again by a substitution/transfer function block as shown on figure 10, ref. Num "182" below ref. Num "180" and produces 8-bit data block output **y'_i**)

and **concatenating said plurality of output signals to present a second output signal** [Column 17, lines 6-8]

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be

patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

12. **Claims 3-6 and 13-16** are rejected under 35 U.S.C. 103(a) as being unpatentable over by **Terry F. Ritter** (hereinafter refereed to as **Ritter**) (U.S. Patent No. 5,623,549) in view of **Eric Sprunk et** al (hereinafter refereed as **Sprunk**) (U.S. Patent No. 5,473,693)

13. **As per claims 3, 5-6,13,15 and 16** **Ritter** discloses establishing a plurality of transfer functions configured to present a plurality of unique symbols as a block output signal responsive to said block input signal;[Column 16, lines 66-Column 17, lines 6;figure 10 ,ref. Num "182"]

Ritter does not explicitly discloses the method wherein said transfer function is a table configured as k columns and 2^k rows where k is a bit width of said block input signal and each said row stores one of said symbols.

However, In the same field of **Sprunk**, discloses many choices of lookup table [column 4, lines 27] such that one of the choices being DES having an S-box is addressed with six-bit width input and each has 4 columns/rows and has 2^4=16 rows/columns as shown on column 4, lines 55-59 and which stores 2^4=64 entries in the matrix.) [See also colum4, lines 49; column 4, lines 55-63]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine table configuration of columns and rows as per teachings of **Sprunk** into the method of transformation as taught by **Ritter**, for the purpose of strengthening the security of the transformation/encryption of data.[see Abstract of Sprunk]

14. **As per claims 4 and 14** the combinations of **Ritter** and **Sprunk** discloses of defining a transformation between an input signal and an output signal as applied to claims 3 and 13 above. Furthermore **Sprunk** discloses the method further comprising the step of extracting said plurality of symbols stored in said tables from a random source configured such that each said symbol has an approximately equal probability of appearance.[Column 4, lines 55-60] (As shown on table on column 4, lines 55-60 and inherently from the DES S-box substitution, the substitution box comprises of a matrix of 64 random values, that is one of the reasons that s-box substitution is considered to be the critical steps in DES algorithm and this is the step more than any thing else give DES secuity]

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S·L
02/09/2005

Gilberto B

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100